CEO CFO

ceocfointerviews.com
All rights reserved!
Issue: February 8, 2016
The Most Powerful Name in Corporate News

Consultants and Implementers of IBM Security Systems Software Providing Expertise on Information Management Analytics and Security Systems

Thomas M. Gibbs III
Co-Founder, Marketing & Sales
SafeITData, LLC

CEOCFO: ***Mr. Gibbs III, what is the vision and the mission at SafeITData?***
Mr. Gibbs III: SafeITData is an IBM Advanced Business partner. We are security software consultants and implementation specialists. We offer value added professional services in that we have the ability to implement several different software product lines of IBM. These products include: Information Management, Analytics and Security Systems software for customers.

CEOCFO: ***Why IBM?***
Mr. Gibbs III: It is very simple; IBM has the only complete security system product portfolio in the world. IBM has security system research centers around the globe. They offer both on premise and cloud offerings. In addition, I am a former IBMer and our entire team of security system architects are also former IBMers.

CEOCFO: ***When might an organization turn to you for services? Is it day one? Why are people coming to you?***
Mr. Gibbs III: A typical client that would come to us is one who wants to review their whole management security strategy. We actually offer a free service in combination with IBM called a Security Controls Review (SCR). That security controls review is conducted by both SafeITData and IBM security architects working together.

The SCR is perfect for an organization looking to mature their security practices, to provide a rapid checkpoint against the top focus controls in the industry, or to provide a baseline review for a new CISO or other security leaders. A company will receive a report that documents its maturity level and specific, 'very next actions' for each control not at the desired state.

CEOCFO: ***What are some of the more common problems that you find? What might you unearth that would surprise most people is a problem?***
Mr. Gibbs III: Most companies do not realize that they are under attack by malware. They may have enterprise grade antivirus software that we think is important. But antivirus software relies on stopping malware that has a signature. A signature means that the malware encountered by the anti-virus software has been seen before somewhere in the globe. The biggest attacks today are called zero-day attacks, where the malware has not been seen previously, and therefore, can easily evade the anti-virus software. Once this software enters a company's infrastructure, they stay on the company's infrastructure until they are able to penetrate applications and start exfiltrating data to the outside attacker. Some of these attacks are five, six or seven months in the making and the companies current security system software does not even know that it is there! This is the number one benefit that a company would come to us for. It is to find malware that they just do not realize is even on their system. In fact, when we install IBM software we usually find several pieces of malware that are attacking a company's infrastructure.

CEOCFO: ***Would you give us an idea of the variety of solutions? How do you decide what is best in any given circumstance?***
Mr. Gibbs III: The security systems solutions are based on what a company may be dealing with. IBM offers software that protects the network, endpoints such as a PC or mobile, applications of the website, legacy system databases, prevents fraud in financial services and delegate's authority as to who is allowed to access any of the company's applications. All of this is then fed into an analytics platform which then prioritizes any threats so that a company can assign personnel to the most important threats first.

Many times a company comes to IBM when they are under attack. IBM helps them with the forensics of understanding how they were attacked and what they need to do. Our focus is preventing the attack before it begins. Therefore, we recommend a multi-layered approach so that a company is not relying on just one piece of software. Not only does IBM's software integrate into its analytics platform, but also IBM allows competitive software to integrate into the platform thru APIs. Therefore, the company does not have to rip and replace their current point solution software out, if it has a good reputation. We feel that that is the best cost effective approach to help the company.

CEOCFO: ***Do companies come to you directly? Do they reach you through IBM?***
Mr. Gibbs III: As a IBM business partner IBM assists us with outbound marketing campaigns to let companies know that we exist. Most of the time companies come to us because we focus on a specific problem in a campaign. They download a white paper or look at a video and then we reach out to them to see if they have a specific problem where we can help them find a solution to. Typically we will recommend that they conduct a Security Controls Review. In that fashion, we become a trusted advisor rather than having a product sale approach. We take a more holistic approach to a company and help them make sure that they have the appropriate management security in place that is best for their company.

CEOCFO: ***Is there a common thread for companies that come to you? Is it size, geography or industry?***
Mr. Gibbs III: The common thread is that a company is concerned that their confidential data will be exposed by a hacker. The cost of a typical data theft today is over $4 million dollars in costs to a company. That number includes the cost of lost records, the cost to improve their security perimeter and the loss of reputation with their customers. The extends beyond the private sector as the Department of Personnel within the US government was hacked last year and millions of records of employees were exposed. This is big business. There are major organizations around the globe where all they want do is to steal a company's confidential information to resell it on the dark web.

> **"Most companies do not realize that they are under attack by malware. They may have enterprise grade antivirus software that we think is important. But antivirus software relies on stopping malware that has a signature. A signature means that the malware encountered by the anti-virus software has been seen before somewhere in the globe. The biggest attacks today are called zero-day attacks, where the malware has not been seen previously, and therefore, can easily evade the anti-virus software."- Thomas M. Gibbs III**

CEOCFO: ***What has changed for you over time? What have you learned along the way that provides a different offering today?***
Mr. Gibbs III: As a former IBMer, I have always been used to promote a brand portfolio sale. We feel that selling the concept of adding value to the customer in addition to a product sale is the way to go today. You really have to provide a holistic approach. I think that is really where we have migrated to over time. There is a major cyber war going on in the marketplace led by sophisticated hackers across the globe. It is the holistic approach in helping a company to develop their overall management security strategy that is the best value added service today.

CEOCFO: ***If a company asks you to review and then take care of the problem do you have an ongoing relationship?***
Mr. Gibbs III: There are several types of relationships. You can have just a one-time relationship where a company asks you to come in and review their current security controls and you might make a recommendation and install software. However, one thing that we are finding today that is very important is that there are not enough trained security resources in the US at companies. That means when we go in and install software, the company may ask us to run and monitor that software for them. Therefore, we offer managed services offerings on just about every product that we recommend, just in the event that a company does not have the appropriate internal resources to monitor the software.

CEOCFO: ***How is business?***
Mr. Gibbs III: Business is really great! This whole marketplace for IBM is growing in excess of twenty percent a year. In some instances, some product lines like application security are growing in excess of 40% a quarter. Most people do not realize that over ninety percent of the applications that are downloaded for their mobile phones are at risk or have been hacked. People that develop applications are so intent on getting them to market that they overlook the ability of hackers to hack their new mobile application. Probably the biggest way in which hackers get into a company's infrastructure is through mobile devices. That is because they are under protected right now. A big push with IBM is to offer endpoint protection and the management of endpoint protection for companies that have a large mobile presence.

CEOCFO: ***Are you surprised that consumers are not demanding better in mobile or are most companies just jumping on to what is available?***
Mr. Gibbs III: By and large, consumers do not realize how vulnerable the mobile marketplace is. I am not sure that there is a whole lot of effort by those companies that have mobile applications to tell consumers that when they download an application that they are actually downloading a potential problem. However, I would say that companies who are in the marketplace to protect mobile applications are keenly aware of the vulnerability of mobile applications and are doing everything that they can to secure mobile apps in today's environment. Therefore, even though the consumers may not have a high awareness, companies do. That is why a product called Application Scanning is in such a high demand. This software examines a mobile application's source code and points out the vulnerabilities in these applications so that they can be fixed.

CEOCFO: ***Why is SafeITData such an important company today?***
Mr. Gibbs III: It is an important company because we can literally save an organization millions of dollars in costs of being hacked. This is something that nobody want to have happen, but when it happens when you take the actual cost of the data loss, the loss of reputation and the cost of remediation; it turns out that the average company, again, is spending well over $4 million. Therefore, we are trying to prevent those kinds of events from occurring. Quite frankly, companies do not usually find out that they have been hacked internally. It is usually from a third party that is doing business from them and it is usually months after the actual hack has taken place that something happens and a third party says, "This is not right, how did my data get out there?" Then they realize, after the fact, after all the damage is done, that there was indeed a breach. We are trying to prevent that and that is a good thing!

Interview conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine

SafeITData, LLC

For more information visit:
www.SafeITData.com

Contact:
Thomas M. Gibbs III
916-652-5520
Tom.Gibbs@SafeITData.com